

Expert Analysis Technology

*The Foundation
for Intelligent
Network
Management*



Network General Corporation delivers intelligent and integrated network analysis solutions that lead the industry. These systems and applications help organizations optimize the performance of heterogeneous LANs, internetworks, and enterprise network environments. Since 1986, the company has engineered the industry's award-winning Protocol Interpretation, standards-based RMON, and artificial intelligence Expert Analysis applications.

Delivering important milestones in true multivendor interoperability and cooperation, Network General's

Sniffer technology is the de facto industry standard. The company maintains qualified sales, service, and support organizations to help customers proactively plan their networks, optimize performance, and achieve maximum network availability. With installations in 90% of Fortune 100 companies and over 3,500 customers worldwide, Network General is the network analysis market share leader.

For more information about Network General's comprehensive products and services, please call 1-800-SNIFFER (1-800-764-3337).

The Foundation for Intelligent Network Management

Network General Corporation leads the industry, delivering intelligent network analysis and monitoring solutions that address evolving trends in computing technology. As businesses increasingly rely on client/server networks to maximize their competitive edge, Network General offers a family of products and services that help solve network problems and maximize network performance.

Network General pioneered Expert Analysis technology in 1991. By placing the intelligence of a network expert into the hands of network professionals, Expert Analysis continues to revolutionize the process of network design, implementation, and management. Expert Analysis forms the foundation for intelligent systems management and helps:

- Improve network performance and decrease downtime
- Identify problems proactively and speed the problem resolution process
- Increase productivity by providing answers, not just data
- Reduce network operating costs and leverage existing hardware

This paper explores the following:

- What is Expert Analysis?
- Expert Solutions to Network Problems
- The Benefits of Expert Analysis
- Network General Expert Analysis Products

What Is Expert Analysis

Network General developed Expert Analysis technology to meet the challenges of managing increasingly complex and constantly changing networks. This innovative, artificial intelligence network analysis software is based on theoretical and prototype work done at Stanford University¹, the University of Massachusetts², and Nippon Telephone and Telegraph (NTT)³. Network General spent several years evaluating, modifying, and adapting various artificial intelligence methodologies to create its industry-leading Expert Analysis technology.

How Does Expert Analysis Work?

Today, Expert Analysis captures packets as they travel across the network. These packets are forwarded to a set of real-time protocol decode modules which then extract information or "network objects" from each packet. These objects store critical information such as the IP address, connection number, or a set of file transfers between two stations. The objects contain packet information about all seven OSI layers.

Objects are the key (see Figure 1, page 3). With Expert Analysis, the system stores the most important information as objects and then uses this object-based information to identify network problems. Object-oriented methods provide both generalized information handling and the ability to adapt to topology- or protocol-specific issues as required.

At the same time, Expert Analysis creates a logical view of the network by determining which devices are communicating with which other devices. The network objects are stored in a "Blackboard Knowledge Base"⁴ and are constantly updated as new information is extracted by the protocol decode modules.

Expert Analysis technology also includes Knowledge Sources that incorporate years of network management experience into the software. Each separate Knowledge Source constantly posts information to the Blackboard and examines it to identify network problems. When a problem is identified, the Knowledge Source generates a symptom and/or diagnosis on the screen for you to act upon.

Moreover, A Knowledge Source can detect a class of problems across many network types by looking for generalized types of problems across protocols. This provides very powerful problem detection in a multivendor, multiprotocol environment. It also makes Sniffer Expert Analysis technology easily extensible to additional network problems. In addition to providing real-time problem identification at all seven OSI layers, Expert Analysis also provides explanations to possible causes for each problem discovered.

1 Hitson, Bruce L. "Knowledge-Based Monitoring and Control of Distributed Systems," Technical Report Number CSL-TR-414, Stanford University, February, 1990.

2 Lesser, V., et al. "A High-Level Simulation Testbed for Cooperative Distributed Problem-Solving," *Computer and Information Science*, University of Massachusetts at Amherst, March, 1981.

3 Sugawara, Toshiharu. "A Cooperative LAN Diagnostic and Observation Expert System," *IEEE Proceedings of the IEEE Phoenix International Conference on Computers and Communication*, 1990, pp. 667-674.

4 Corkill, Daniel. "Blackboard Systems," *AI Expert*, September, 1991, pp. 41-47.

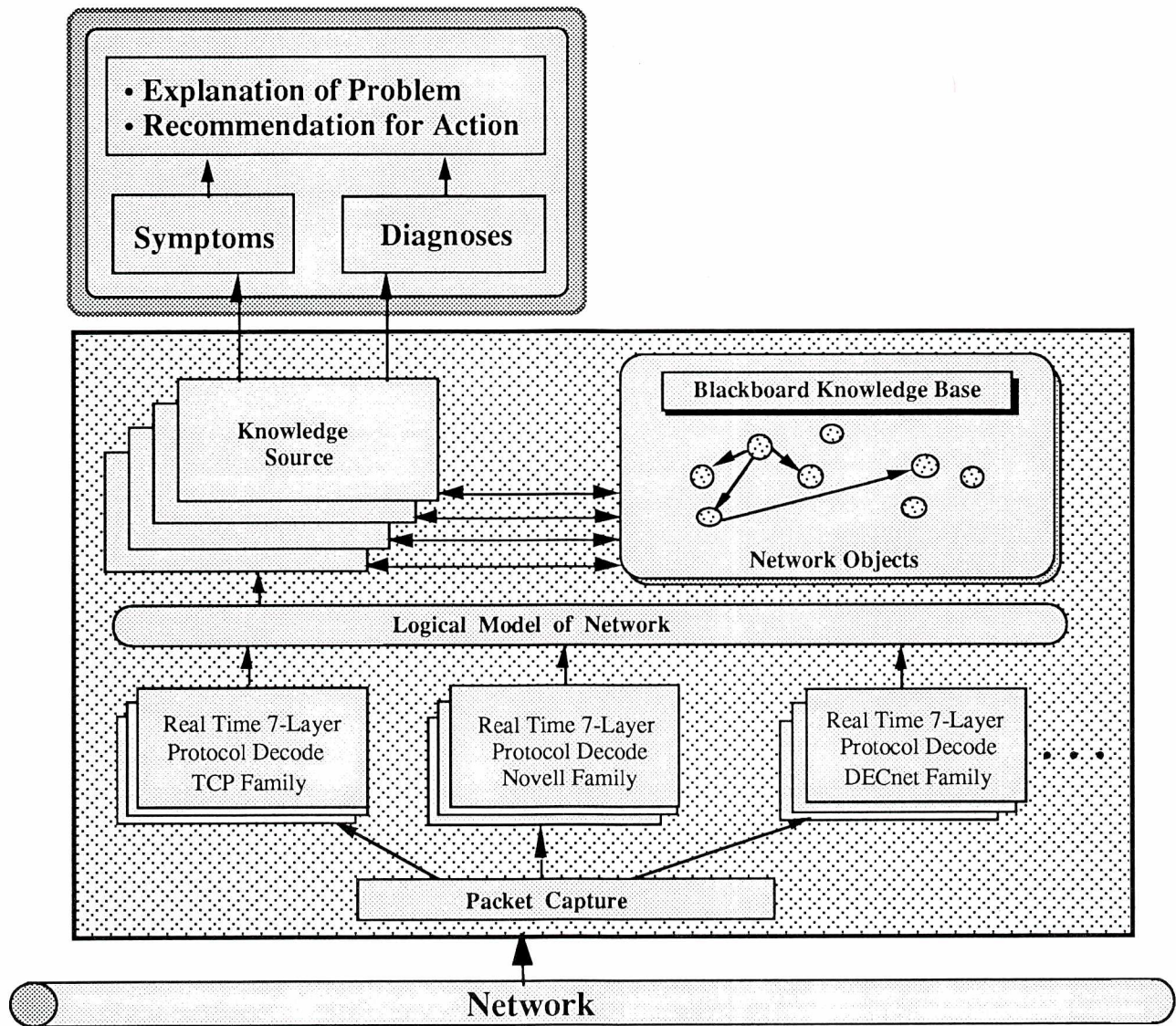


Figure 1: Expert Sniffer technology extracts network objects from each packet to identify network problems

Revolutionary Management Technology

Expert Analysis technology puts years of network troubleshooting experience into your hands. Unlike other network troubleshooting tools, Network General Sniffer products use the artificial intelligence capabilities of Expert Analysis to automatically identify network problems. This industry-leading technology allows you to take advantage of the collective expertise amassed through years of Network General's focused network analysis efforts.

Expert Analysis technology solves many common network problems at all seven layers of the OSI model. To understand how, think of a network analyzer as an X-ray machine. An X-ray shows the bone structure of the patient, but a specialized technician is still required

to interpret the findings, and a doctor is needed to make the final diagnosis.

Expert Analysis combines the roles of the X-ray machine, technician, and doctor into one. Expert Analysis creates a system that identifies, interprets, and diagnoses network problems and performance irregularities. Because Expert Analysis does this work automatically, you can quickly correct existing problems, proactively identify potential problems, and maximize network performance.

Expert Analysis helps automate the process of solving network problems in high-performance environments. Figures 2 and 3 depict a typical problem-solving scenario using Protocol Interpretation and Expert Analysis applications.

SUMMARY	Delta T	DST	SRC	
4032	0.0014	Client 5	*Server 6	NCP R OK
4033	0.0157	Server 6	*Client 5	NCP C F=5751 Read 2 at 287426
4034	0.0014	Client 5	*Server 6	NCP R OK 2 bytes read
4035	0.0033	Server 6	*Client 5	NCP C F=5751 Read 6 at 287428
4036	0.0014	Client 5	*Server 6	NCP R OK 6 bytes read
4037	0.0032	Server 6	*Client 5	NCP C F=5751 Read 310 at 287434
4038	0.0017	Client 5	*Server 6	NCP R OK 310 bytes read
4039	0.0010	Server 6	*Client 5	NCP C F=5751 Read 121 at 287744
4040	0.0015	Client 5	*Server 6	NCP R OK 121 bytes read
4041	0.0106	Server 6	*Client 5	NCP C F=5751 Read 2 at 447755
4042	0.0013	Client 5	*Server 6	NCP R OK 2 bytes read
4043	0.0032	Server 6	*Client 5	NCP C F=5751 Read 86 at 447757
4044	0.0015	Client 5	*Server 6	NCP R OK 86 bytes read
4045	0.0029	Server 6	*Client 5	NCP C F=5751 Read 669 at 447843
4046	0.0020	Client 5	*Server 6	NCP R OK 669 bytes read
4047	0.0008	Server 6	*Client 5	NCP C F=5751 Read 247 at 448512
4048	0.0015	Client 5	*Server 6	NCP R OK 247 bytes read
4050	0.0575	Server 6	*Client 5	NCP C F=5751 Read 2 at 19223
4051	0.0014	Client 5	*Server 6	NCP R OK 2 bytes read
4052	0.0032	Server 6	*Client 5	NCP C F=5751 Read 6 at 19225
Frame 4032 of 5847				

Figure 2: Protocol Interpretation Application

This screen shows a Novell NetWare client reading a file from the server. By examining the read byte sizes and calculating the time between packets, you can determine that the transaction throughput is low.

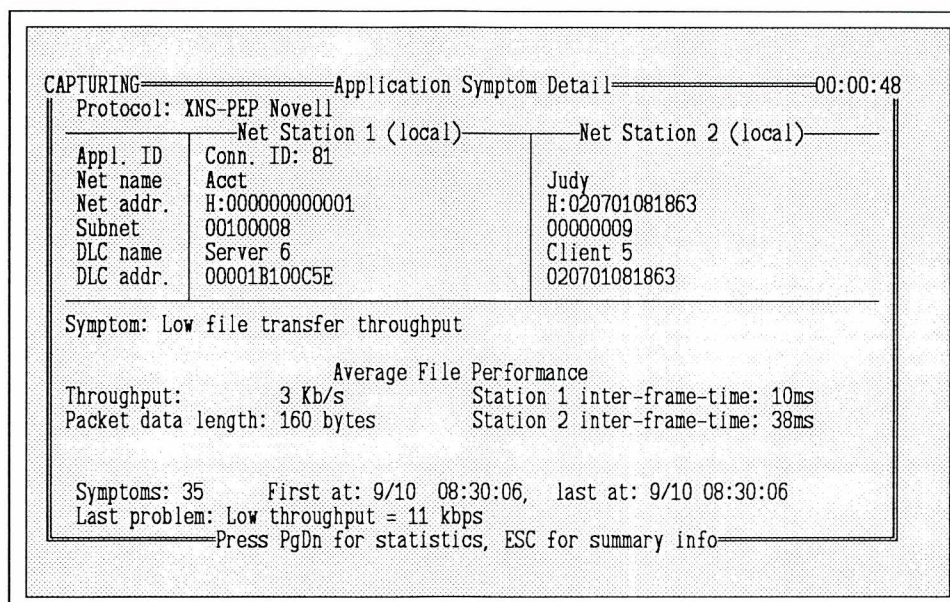


Figure 3: Expert Sniffer Technology

Expert Analysis observes the file transfer shown previously in Figure 2 and automatically determines that the file throughput is low. No detailed calculations are required by the network manager. In addition, Expert Analysis discovers a wealth of statistical information (such as the network names of the client and server), enabling faster pinpointing of problem areas. The statistical information supports the Expert Analysis diagnosis of low throughput. Using this Expert Analysis information, you can focus your troubleshooting efforts for faster problem resolution.

Expert Solutions to Network Problems

Expert Analysis provides you with three types of information:

- Symptoms
- Diagnoses
- Explanations

In Figures 4 through 6, Expert Analysis automatically identifies a router configuration problem. Figure 4 explains the problem. Figure 5 draws a context-sensitive network diagram showing how a router is used for communication between two stations on the same local network. Figure 6 offers possible causes of the problem and provides suggestions for corrective action.

Symptoms

As traffic passes over individual LAN and internetwork segments, Expert Analysis examines the network for unusual activities called symptoms. By itself, a symptom is not necessarily a fault, but it could indicate a potential network problem. Symptoms are events you might want to investigate before they become serious problems. For example, a single file retransmission is not necessarily a problem because the network continues to function and users continue to perform their work. However, when file retransmissions happen multiple times in a row on the same file, or retransmit repeatedly over a few seconds, network performance may suffer.

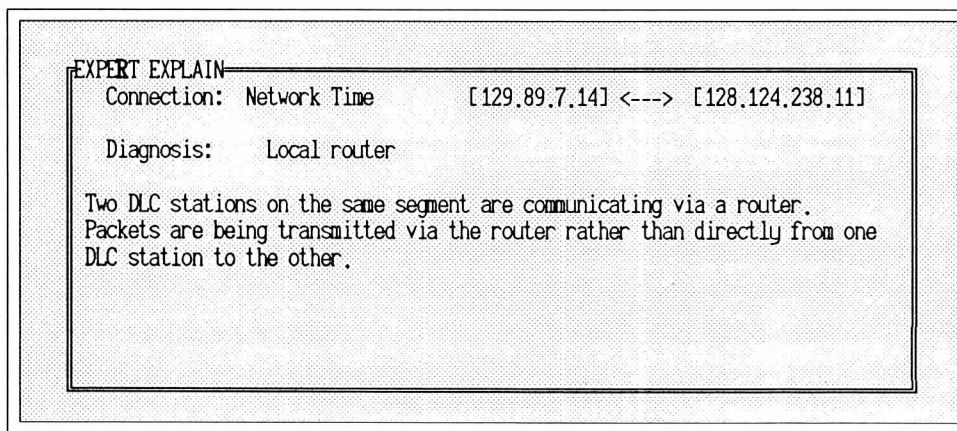


Figure 4: Expert Analysis identifies the symptoms, diagnoses problems, and provides explanations automatically

Diagnoses

A diagnosis highlights something that, in the judgment of the Expert Analysis software, you should act on. Expert Analysis automatically provides diagnoses when a symptom repeats itself frequently

(such as excessive file retransmissions) or where there is a single instance of a major network problem (such as a duplicate network address). Diagnoses highlight solutions to problems that may impact network performance.

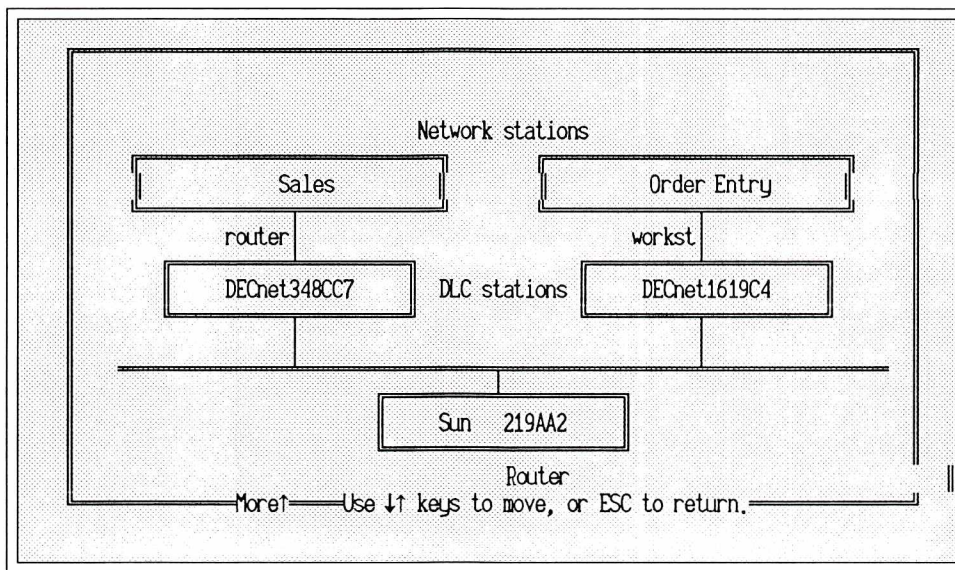


Figure 5: Expert Analysis provides diagrams that illustrate and explain network problems

Explanations

For each symptom and diagnosis, Expert Analysis creates a network-specific explanation of the condition and automatically recommends possible solutions. Based on the symptoms and diagnoses, Expert Analysis automatically offers explanations that recommend possible corrective action.

Expert Analysis delivers symptoms, diagnoses, and explanations for a wide variety of network problems including:

- **Internetworking Problems**

Expert Analysis pinpoints duplicate network addresses. The nodes involved are identified automatically. Router misconfigurations are also highlighted to help minimize WAN bandwidth charges.

- **Performance Bottlenecks**

Expert Analysis helps detect multiple file retransmissions, non-responsive stations, and slow servers that can cause performance bottlenecks.

- **Protocol Violations**

Expert Analysis recognizes non-standard protocol activity such as missing acknowledgments and window size problems, and suggests solutions for protocol problems.

- **Physical-Layer Problems**

Expert Analysis speeds the process of identifying and solving Ethernet and token ring lower-layer problems, including congestion and ring beaconing.

Possible causes:

1. The router table may be improperly configured. If this is the case, reconfigure the router table so that the stations can communicate with each other directly.
2. The router may be used for security purposes, to control access to particular parts of the network.
3. The router may be performing gateway type functions, such as protocol translation at the application level.
4. A device that is new to the network is sending frames through a router because it has not yet become aware of the direct route to a local station.

Figure 6: Expert Analysis offers explanations about possible causes of network problems

The Benefits of Expert Analysis

In order to effectively solve network problems and improve network performance, Network General's Expert Analysis technology dissects and analyzes real-time data moving at high speeds across the network at all seven OSI layers. The benefits of this intelligent network analysis solution include:

Proactive Network Management

Expert Analysis keeps your network operative by automatically forewarning you of problems before they affect end users. Expert Analysis pinpoints network problems at all seven OSI layers and suggests solutions in real time to help return your network to peak performance levels. With the Network General® Reporter application, you can use Expert Analysis data to generate real-time reports. Use these reports to forecast application requirements and justify equipment purchases so your network continues to operate efficiently.

Automatic Problem Identification

Expert Analysis gets to the underlying cause of problems on Ethernet and token ring LAN segments, as well as bridged and routed internetworks. From the physical through the application layers, Expert Analysis technology automatically provides detailed, real-time diagnoses and English explanations of many common network problems while traffic is moving across the network. This fast identification and analysis of problems translates directly into increased performance and reduced network downtime.

Optimized Network Investments

Understanding a network's configuration is critical to optimizing your investment in network components. Expert Analysis automatically learns a network's logical configuration and constantly updates it in real time. First, Expert Analysis learns station names, routing paths, and configuration information. Then, Expert Analysis applies this information automatically to pinpoint network inefficiencies. Using Expert Analysis information, you can create in-depth reports with the Network General Reporter application. Use this information to track your network's performance, analyze historical trends, and configure your network for peak performance.

Network General Expert Analysis Products

Network General engineered the industry's premier Expert Analysis software to help you resolve problems on mission-critical segments more quickly. Today, our Sniffer® systems and tools continue to address your network management needs with quality analysis solutions that provide complete coverage of your network segments. Choose from a wide range of Network General products that offer scalable and integrated solutions to keep your network up and running efficiently.

Distributed Sniffer System®

The Distributed Sniffer System (DSS) is a comprehensive network analysis and monitoring system that delivers Expert Analysis technology and Remote Monitoring (RMON) to quickly resolve distributed network problems from a central location. Using DSS, you can also troubleshoot LAN communications over internetworks, as well as Ethernet and token ring segments.

For organizations that rely on client/server applications running over a web of LANs and WANs, DSS aids in baselining, trend analysis, performance tuning, and problem resolution from a single site. Network General developed DSS with a range of monitoring and analysis components for managing distributed client/server networks from end to end.

Network General continues to enhance DSS to broaden Expert Analysis coverage for your distributed network. In addition to integrating Expert Analysis with RMON, DSS integrates with popular network management systems. Today, DSS provides Expert Analysis capabilities in the most popular UNIX environments and on the most powerful network management systems in the industry such as HP OpenView, IBM NetView, and SunNet Manager. Consequently, DSS enables you to optimize your existing hardware investments and manage your distributed networks from a central location.

Expert Sniffer® Network Analyzer

By putting years of network troubleshooting experience into your hands, Expert Sniffer Network Analyzers deliver portable, practical, problem-solving solutions. Today, an expanded line of Sniffer products connects to more physical topologies and interprets more protocols than any other portable analyzer available.

Expert Sniffer Network Analyzers for Ethernet, token ring, internetwork, and FDDI topologies use an intuitive menu and command system. Designed to run on industry standard PCs, rather than expensive proprietary hardware, Expert Sniffer Network Analyzers are ready to solve network problems right out of the box.

Notebook Sniffer® Analyzer

To make troubleshooting easier for field service personnel, Network General introduced a new generation of flexible network analysis solutions that utilize Expert Analysis technology. Notebook Sniffer Analyzers use the Personal Computer Memory Card International Association (PCMCIA) standard and run on a wide variety of notebook PC platforms.

Expert Sniffer® Internetwork Analyzer

With this portable tool, you can directly manage bandwidth costs. By providing a comprehensive view of communications traveling over internetwork links, Expert Sniffer Internetwork Analyzers pinpoint network bottlenecks and offer recommendations to improve bandwidth efficiency, application throughput, and response times.

The Expert Sniffer Internetwork Analyzer resolves complex internetwork issues encountered when running LAN protocols over bridged and routed networks. Expert Analysis displays Expert-level information about LAN protocols running over leased line, frame relay, and X.25 internetworks.

Network General protects your investment in Distributed Sniffer System components and portable Expert Sniffer Network Analyzers. These products will continue to support future enhancements to Expert Analysis technology by means of a simple software upgrade.

Conclusion

Network General's industry-leading Expert Analysis technology forms an intelligent base for developing powerful network analysis applications in multivendor, multiprotocol environments. Expert Analysis revolutionizes the way you manage networks by:

- Proactively finding problems to maximize network performance
- Preventing costly network downtime
- Shortening time to problem resolution
- Increasing productivity by providing answers, not just data
- Reducing network operating costs through more efficient planning and higher network performance

To address the challenge of increasing network complexity, Network General continuously incorporates new problem-solving intelligence into Expert Analysis. Ongoing enhancements to Expert Analysis technology offer insurance that you can address new problems in your network environments. Pioneering the next generation of intelligent network management, Expert Analysis will address multisegment troubleshooting where correlated problem identification is crucial.

By combining our network expertise with the experience of our customers and other industry leaders, Network General consistently develops state-of-the-art solutions. Key industry influentials acknowledge Network General's leadership in the network analysis market. With this commitment to enhance, extend, and build on existing Expert Analysis technology, you can rely on Network General's cumulative knowledge base to help manage growing and changing networks.

**Please contact your Network General
sales representative or call
1-800-Sniffer (1-800-764-3337)
for further information on the industry's
leading Expert Analysis technology.**

**Thank you for your interest in
Network General.**

Further Reading

1. Corkill, Daniel. "Blackboard Systems," *AI Expert*, September, 1991, pp. 41-47.
2. Sugawara, Toshiharu. A Cooperative LAN Diagnostic and Observation Expert System, *IEEE Proceedings of the IEEE Phoenix International Conference on Computers and Communication*, 1990, pp. 667-674.
3. Hitson, Bruce L. "Knowledge-Based Monitoring and Control of Distributed Systems," Technical Report Number CSL-TR-90-414, Stanford University, February, 1990.
4. Lesser, V. et. al. The HEARSAY-II speech understanding system: integrating knowledge to resolve uncertainty, *Computing Surveys*, 1980, pp. 213-253.
5. Nii, H. Penny. *Blackboard Systems*, Report KSL 86-18, Knowledge Systems Laboratory, Stanford University, June, 1986.
6. Waterman, Donald A. *A Guide To Expert Systems*, Addison-Wesley Publishing, Reading, MA, 1986.
7. Lesser, V. et. al. "A High-Level Simulation Test Bed for Cooperative Distributed Problem-Solving," *Computer and Information Science*, University of Massachusetts at Amherst, March, 1981.
8. Winston, Patrick Henry. *Artificial Intelligence*, Addison-Wesley Publishing, Reading, MA, 1984.

**Corporate Headquarters****Network General Corporation**

4200 Bohannon Drive
Menlo Park, CA 94025 USA
TEL: (415) 473-2000
FAX: (415) 321-0855

U.S. Sales Offices

Menlo Park, CA (800) 846-6601

Eastern Region

Wakefield, MA (617) 224-1244
Red Bank, NJ (908) 758-0062
Rockville Center, NY (516) 766-4100
Westlake, OH (216) 892-1330
Dunn Loring, VA (703) 641-0074

Central Region

Atlanta, GA (404) 491-3800
Oakbrook Terrace, IL (708) 574-5770
Carrollton, TX (214) 386-6384

Western Region

Phoenix, AZ (602) 598-0335
Anaheim, CA (714) 939-9188
Santa Clara, CA (408) 982-1910
Westlake Village, CA (818) 597-9012

Asia

Network General Asia
111 Northbridge Road #11-04
Peninsula Plaza, Singapore
TEL: (65) 336-0431
FAX: (65) 339-5291

Australia

Network General Australia PTY Ltd.
Level 20, 99 Walker Street
North Sydney, NSW, 2060 Australia
TEL: (61) 2-911-7770
FAX: (61) 2-911-7750

Europe**Belgium**

Network General Europe N.V.
Belgicastraat 4
B-1930 Zaventem, Belgium
TEL: (32) 2-725-6030
FAX: (32) 2-725-6639

France

Network General France S.A.R.L.
Atria, 21 Avenue Edouard Belin
F-92566 Rueil Malmaison
Cedex, France
TEL: (33) 1-47-16-9900
FAX: (33) 1-47-16-9907

Germany

Network General GmbH
Mettmanner Strasse 24
D-40233 Duesseldorf, Germany
TEL: (49) 211-98-4050
FAX: (49) 211-730-8839

Switzerland

Network General NGC AG
Lerzenstrasse 21
CH-8953 Dietikon Switzerland
TEL: (41) 1-742-2550
FAX: (41) 1-742-2554

North America**Canada**

Network General Canada, Ltd.
9225 Leslie Street, Unit 7
Richmond Hill, Ontario L4B 3H6
Canada
TEL: (905) 882-7905
FAX: (905) 882-9454

South America**Brazil**

Network General do Brasil
Avenida Paulista, 1439, Cj. 52
01311-200 - Sao Paulo - S.P., Brazil
TEL: (55) 11-289-7666
FAX: (55) 11-289-6215

Latin America

Network General Latin America &
Caribbean
3609 Cleveland Street
Hollywood, FL 33021
TEL: (305) 981-3388
FAX: (305) 981-9470

GSA Schedule Number—GSOOK92AGS6109 PS08

Network General, Sniffer, SniffMaster, Distributed Sniffer System, and LANGuru are registered trademarks of Network General Corporation. Sniffer University is a trademark of Network General Corporation. Foundation Manager and Cornerstone Probe are trademarks of ProTools, Inc. ProTools is a wholly owned subsidiary of Network General Corporation. All other registered and unregistered trademarks above are the sole property of their respective owners. All specifications may be changed without notice.
© Copyright 1994 Network General Corporation. All rights reserved.

Printed on recycled paper. P/N 24148-004 10/94

Forward product suggestions to Network General via the Internet to: suggestions@ngc.com

**Network General products
are available from sales
offices and distributors
worldwide.**